FortiOS - Release Notes

Version 5.6.5

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

June 21, 2018
FortiOS 5.6.5 Release Notes
01-565-495894-20180621

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-06-21	Initial release.

Introduction

This document provides the following information for FortiOS 5.6.5 build 1600:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Limitations

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 5.6.5 supports the following models.

FortiGate	FG-30D, FG-30E, FG-30E_3G4G_INTL, FG-30E_3G4G_NAM, FG-30D-POE, FG-50E, FG-51E, FG-52E, FG-60D, FG-60D-POE, FG-60E, FG-60E-DSL, FG-60E-POE, FG-61E, FG-70D, FG-70D-POE, FG-80C, FG-80CM, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90D, FG-90D-POE, FG-90E, FG-91E, FG-92D, FG-94D-POE, FG-98D-POE, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200D, FG-200D-POE, FG-200E, FG-201E, FG-240D, FG-240D-POE, FG-280D-POE, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600C, FG-600D, FG-800C, FG-800D, FG-900D, FG-1000C, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3240C, FG-3600C, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001C, FG-5001D, FG-5001E, FG-5001E1
FortiWiFi	FWF-30D, FWF-30E, FWF-30E_3G4G_INTL, FWF-30E_3G4G_NAM, FWF-30D-POE, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60D, FWF-60D-POE, FWF-60E, FWF-60E-DSL, FWF-61E, FWF-80CM, FWF-81CM, FWF-90D, FWF-90D-POE, FWF-92D
FortiGate Rugged	FGR-30D, FGR-35D, FGR-60D, FGR-90D
FortiGate VM	FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-OPC, FG-SVM, FG-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN
FortiOS Carrier	FortiOS Carrier 5.6.5 images are delivered upon request and are not available on the customer support firmware download page.

VXLAN supported models

The following models support VXLAN.

FortiGate	FG-30E, FG-30E-MI, FG-30E-MN, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DLS, FG-60E-MC, FG-60E-MI, FG-60E-POE, FG-60EV, FG-61E, FG-80D, FG-80E, FG-80E-POE, FG-81E, FG-81E-POE, FG-90E, FG-91E, FG-92D, FG-100D, FG-100E, FG-100EF, FG-101E, FG-140D, FG-140D-POE, FG-140E, FG-140E-POE, FG-200E, FG-201E, FG-300D, FG-300E, FG-301E, FG-400D, FG-500D, FG-500E, FG-501E, FG-600D, FG-800D, FG-900D, FG-1000D, FG-1200D, FG-1500D, FG-1500DT, FG-2000E, FG-2500E, FG-3000D, FG-3100D, FG-3200D, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-3960E, FG-3980E, FG-5001D, FG-5001E, FG-5001E1
FortiWiFi	FWF-30E, FWF-30E-MI, FWF-30E-MN, FWF-50E, FWF-50E-2R, FWF-51E, FWF-60E, FWF-60E-DSL, FWF-60E-MC, FWF-60E-MI, FWF-60EV, FWF-61E
FortiGate Rugged	FGR-30D, FGR-30D-A, FGR-35D
FortiGate VM	FG-VM64, FG-VM64-AWS, FG-VM64-AWSONDEMAND, FG-VM64-AZURE, FG-VM64-AZUREONDEMAND, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-KVM, FG-VM64-NPU, FG-VM64-OPC, FG-VM64-SVM, FG-VM64-VMX, FG-VM64-XEN
Pay-as-you-go images	FOS-VM64, FOS-VM64-KVM, FOS-VM64-XEN

What’s new in FortiOS 5.6.5

For a list of new features and enhancements that have been made in FortiOS 5.6.5, see the *What’s New for FortiOS 5.6.5* document in the Fortinet Document Library.

Special Notices

Built-in certificate

New FortiGate and FortiWiFi D-series and above are shipped with a built in Fortinet_Factory certificate that uses a 2048-bit certificate with the 14 DH group.

FortiGate and FortiWiFi-92D hardware limitation

FortiOS 5.4.0 reported an issue with the FG-92D model in the *Special Notices > FG-92D High Availability in Interface Mode* section of the release notes. Those issues, which were related to the use of port 1 through 14, include:

- PPPoE failing, HA failing to form.
- IPv6 packets being dropped.
- FortiSwitch devices failing to be discovered.
- Spanning tree loops may result depending on the network topology.

FG-92D and FWF-92D do not support STP. These issues have been improved in FortiOS 5.4.1, but with some side effects with the introduction of a new command, which is enabled by default:

```
config global
   set hw-switch-ether-filter <enable | disable>
```

When the command is enabled:

- ARP (0x0806), IPv4 (0x0800), and VLAN (0x8100) packets are allowed.
- BPDUs are dropped and therefore no STP loop results.
- PPPoE packets are dropped.
- IPv6 packets are dropped.
- FortiSwitch devices are not discovered.
- HA may fail to form depending the network topology.

When the command is disabled:

- All packet types are allowed, but depending on the network topology, an STP loop may result.

FG-900D and FG-1000D

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip.

FortiGate-VM 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.5, FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

FortiClient profile changes

With introduction of the Fortinet Security Fabric, FortiClient profiles will be updated on FortiGate. FortiClient profiles and FortiGate are now primarily used for Endpoint Compliance, and FortiClient Enterprise Management Server (EMS) is now used for FortiClient deployment and provisioning.

The FortiClient profile on FortiGate is for FortiClient features related to compliance, such as Antivirus, Web Filter, Vulnerability Scan, and Application Firewall. You may set the *Non-Compliance Action* setting to *Block* or *Warn*. FortiClient users can change their features locally to meet the FortiGate compliance criteria. You can also use FortiClient EMS to centrally provision endpoints. The EMS also includes support for additional features, such as VPN tunnels or other advanced options. For more information, see the *FortiOS Handbook – Security Profiles*.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

FortiExtender support

Due to OpenSSL updates, FortiOS 5.6.5 cannot manage FortiExtender 3.2.0 or earlier. If you run FortiOS 5.6.5 with FortiExtender, you must use a newer version of FortiExtender such as 3.2.1 or later.

Using ssh-dss algorithm to log in to FortiGate

In version 5.4.5 and later, using `ssh-dss` algorithm to log in to FortiGate via SSH is no longer supported.

Upgrade Information

Upgrading to FortiOS 5.6.5

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

If you are upgrading from version 5.6.2, this caution does not apply.
Before upgrading, ensure that port 4433 is not used for `admin-port` or `admin-sport` (in `config system global`), or for SSL VPN (in `config vpn ssl settings`).
If you are using port 4433, you must change `admin-port`, `admin-sport`, or the SSL VPN port to another port number before upgrading.

After upgrading, if FortiLink mode is enabled, you must manually create an explicit firewall policy to allow RADIUS traffic for 802.1x authentication from the FortiSwitch (such as from the FortiLink interface) to the RADIUS server through the FortiGate.

Physical interface inclusion in zones

Upgrading from 5.6.3 or later removes all of the members of a zone if the zone contains a physical interface and at least one of that physical interface's VLAN interfaces is removed. For example:

Before Upgrade:

```
config system zone
   edit "Trust"
   set interface "port1" "Vlan01" "Vlan02" "Vlan03"
next
```

After Upgrade:

```
config system zone
   edit "Trust"
next
```

Remove "port1" from the list and the upgrade will retain the VLANs.

Conditions when physical zone members are removed:

- If a physical interface has a VLAN associated (regardless of whether they are in the same zone or any zone)

Conditions when VLAN zone members are removed:

- If the parent physical interface is also set on a zone

You can use the following options to prepare for the upgrade:

- Use only physical interfaces that have no VLAN associations

  Or:
- Create new VLANs in place of current physical interface zone members, and remove all physical zone members from zones using only the associated, new VLAN entries.

Security Fabric upgrade

FortiOS 5.6.5 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 5.6.1
- FortiClient 5.6.0
- FortiClient EMS 1.2.2
- FortiAP 5.4.2 and later
- FortiSwitch 3.6.2 and later

Upgrade the firmware of each product in the correct order. This maintains network connectivity without the need to use manual steps.

Before upgrading any product, you must read the *FortiOS Security Fabric Upgrade Guide*.

FortiClient profiles

After upgrading from FortiOS 5.4.0 to 5.4.1 and later, your FortiClient profiles will be changed to remove a number of options that are no longer supported. After upgrading, review your FortiClient profiles to make sure they are configured appropriately for your requirements and either modify them if required or create new ones.

The following FortiClient Profile features are no longer supported by FortiOS 5.4.1 and later:

- Advanced FortiClient profiles (XML configuration).
- Advanced configuration, such as configuring CA certificates, unregister option, FortiManager updates, dashboard Banner, client-based logging when on-net, and Single Sign-on Mobility Agent.
- VPN provisioning.
- Advanced AntiVirus settings, such as Scheduled Scan, Scan with FortiSandbox, and Excluded Paths.

- Client-side web filtering when on-net.
- iOS and Android configuration by using the FortiOS GUI.

With FortiOS 5.6.5, endpoints in the Security Fabric require FortiClient 5.6.0. You can use FortiClient 5.4.3 for VPN (IPsec VPN, or SSL VPN) connections to FortiOS 5.6.2, but not for Security Fabric functions.

It is recommended that you use FortiClient Enterprise Management Server (EMS) for detailed Endpoint deployment and provisioning.

FortiGate-VM 5.6 for VMware ESXi

Upon upgrading to FortiOS 5.6.5, FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- VDOM parameters/settings
- admin user account
- session helpers
- system access profiles

If you have long VDOM names, you must shorten the long VDOM names (maximum 11 characters) before downgrading:

1. Back up your configuration.
2. In the backup configuration, replace all long VDOM names with its corresponding short VDOM name.
   For example, replace `edit <long_vdom_name>/<short_name>` with `edit <short_name>/<short_name>`.
3. Restore the configuration.
4. Perform the downgrade.

Amazon AWS enhanced networking compatibility issue

With this new enhancement, there is a compatibility issue with older AWS VM versions. After downgrading a 5.6.5 image to an older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover

the downgraded image.

When downgrading from 5.6.5 to older versions, running the enhanced nic driver is not allowed. The following AWS instances are affected:

- C3
- C4
- R3
- I2
- M4
- D2

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager on Hyper-V 2012. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiOS 5.6.5 support

The following table lists 5.6.5 product integration and support information:

Web Browsers	• Microsoft Edge 38 • Mozilla Firefox version 54 • Google Chrome version 59 • Apple Safari version 9.1 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge 40 • Microsoft Internet Explorer version 11 • Mozilla Firefox version 53 • Google Chrome version 58 • Apple Safari version 10 (For Mac OS X) Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Security Fabric upgrade on page 10. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Security Fabric upgrade on page 10. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient Microsoft Windows	See important compatibility information in Security Fabric upgrade on page 10. • 5.6.1 If FortiClient is managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.
FortiClient Mac OS X	See important compatibility information in Security Fabric upgrade on page 10. • 5.6.0 If FortiClient is managed by a FortiGate, you must upgrade FortiClient before upgrading FortiGate.
FortiClient iOS	• 5.4.3 and later
FortiClient Android and FortiClient VPN Android	• 5.4.1 and later

FortiAP	• 5.4.2 and later • 5.6.0
FortiAP-S	• 5.4.3 and later • 5.6.0
FortiSwitch OS (FortiLink support)	• 3.6.2 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C.
FortiSandbox	• 2.3.3 and later

Fortinet Single Sign-On (FSSO)	• 5.0 build 0267 and later (needed for FSSO agent support OU in group filters)
	  • Windows Server 2016 Datacenter
	  • Windows Server 2016 Standard
	  • Windows Server 2008 (32-bit and 64-bit)
	  • Windows Server 2008 R2 64-bit
	  • Windows Server 2012 Standard
	  • Windows Server 2012 R2 Standard
	  • Novell eDirectory 8.8
	FSSO does not currently support IPv6.

FortiExtender	• 3.2.1 and later See FortiExtender support on page 8.
AV Engine	• 5.247
IPS Engine	• 3.00522
Virtualization Environments	
Citrix	• XenServer version 5.6 Service Pack 2 • XenServer version 6.0 and later
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Microsoft	• Hyper-V Server 2008 R2, 2012, and 2012 R2
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, and 6.5  FortiGate-VM v5.6 for VMware ESXi (all models) no longer supports the VMXNET2 vNIC driver.

VM Series - SR-IOV	The following NIC chipset cards are supported: • Intel 82599 • Intel X540 • Intel X710/XL710

Language support

The following table lists language support information.

Language support

Language	GUI
English	✔
Chinese (Simplified)	✔
Chinese (Traditional)	✔
French	✔
Japanese	✔
Korean	✔
Portuguese (Brazil)	✔
Spanish	✔

SSL VPN support

SSL VPN standalone client

The following table lists SSL VPN tunnel client standalone installer for the following operating systems.

Operating system and installers

Operating System	Installer
Linux CentOS 6.5 / 7 (32-bit & 64-bit) Linux Ubuntu 16.04	2336. Download from the Fortinet Developer Network https://fndn.fortinet.net.

Other operating systems may function correctly, but are not supported by Fortinet.

SSL VPN standalone client no longer supports the following operating systems:

- Microsoft Windows 7 (32-bit & 64-bit)
- Microsoft Windows 8 / 8.1 (32-bit & 64-bit)
- Microsoft Windows 10 (64-bit)
- Virtual Desktop for Microsoft Windows 7 SP1 (32-bit)

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit) Microsoft Windows 8 / 8.1 (32-bit & 64-bit)	Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Microsoft Windows 10 (64-bit)	Microsoft Edge Microsoft Internet Explorer version 11 Mozilla Firefox version 54 Google Chrome version 59
Linux CentOS 6.5 / 7 (32-bit & 64-bit)	Mozilla Firefox version 54
Mac OS 10.11.1	Apple Safari version 9 Mozilla Firefox version 54 Google Chrome version 59
iOS	Apple Safari Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

SSL VPN host compatibility list

It is recommended to verify the accuracy of the GUID for the software you are using for SSL VPN host check. The following Knowledge Base article at http://kb.fortinet.com/ describes how to identify the GUID for antivirus and firewall products: How to add non listed 3rd Party AntiVirus and Firewall product to the FortiGate SSL VPN Host check.

After verifying GUIDs, you can update GUIDs in FortiOS using this command:

```
config vpn ssl web host-check-software
```

Following is an example of how to update the GUID for AVG Internet Security 2017 on Windows 7 and Windows 10 by using the FortiOS CLI.

The GUIDs in this example are only for AVG Internet Security 2017 on Windows 7 and Windows 10. The GUIDs might be different for other versions of the software and other operation systems.

To update GUIDs in FortiOS:

1. Use the `config vpn ssl web host-check-software` command to edit the `AVG-Internet-Security-AV` variable to set the following GUID for AVG Internet Security 2017: `4D41356F-32AD-7C42-C820-63775EE4F413`.
2. Edit the `AVG-Internet-Security-FW` variable to set the following GUID: `757AB44A-78C2-7D1A-E37F-CA42A037B368`.

Resolved Issues

The following issues have been fixed in version 5.6.5. For inquires about a particular bug, please contact Customer Service & Support.

Authentication

Bug ID	Description
474833	Newly generated *Fortinet_CA_SSL* certificate reverts back to previous version after reboot on FG-61E with VDOMs.
476692	Multiple `FNBAMD` crashes.
491175, 491241	`diag test application fnbamd 1` causes `fnbamd` to go into an idle state and authentication failure.
491235	New diag command `diag test app wad 13`.

AV

Bug ID	Description
441739	Enabling AV breaks web connection to license server.
461707	FortiGate cannot generate replacement messages properly when FortiGate set block oversize for SMTP.

Connectivity

Bug ID	Description
460617	GUI FortiGuard *Check Again* button doesn't work as expected due to FortiGuard service 8888/53 incorrectly routed.
467733	All users will disconnect automatically and not be able to connect again (it will show password is incorrect).
477135	Updates of FortiGuard are causing CPU spikes which slows down regular traffic.

DLP

Bug ID	Description
496255	Some XML-based MS Office files are recognized as ZIP file.

DNS Filter

Bug ID	Description
470650	DNS filter getting purged by FortiManager when not used in a policy because FortiGate DNS filter does not contain static entry.
478076	DNS source IP setting is ignored in case communication with SDNS server goes over IPsec tunnel interface.

Endpoint Control

Bug ID	Description
473248	FortiClient blocks all navigation with *APPCTRL* profile when registered to FortiGate.
479672	FortiTelemetry not blocking VIP.

FIPS-CC

Bug ID	Description
463211	When alarm is enabled in FIPS mode, the console hangs and the `getty` process uses very high CPU usage.

Firewall

Bug ID	Description
470167	Session state shows "dirty" even if the policy setting had not been changed after session established.

FortiGate 500D

Bug ID	Description
403449	FortiGate 500D has some issue with FINISAR transceiver.

FortiSwitch-Controller

Bug ID	Description
408082	Operating a dedicated hardware switch into FortiLink changes STP from *enable* to *disable* in a hidden way.
477885	FSW Security Policy – RADIUS configuration not pushed to FSW if `source-ip` is specified. Workaround: configure a separate RADIUS server without `source-ip` parameter and use it in the FSW security policy.
482835	The `cu_acd` process uses high CPU on FG-90D.

FortiView

Bug ID	Description
441835	Drill down a `auth-failed` wifi client entry in "Failed Authentication" could not display detail logs when CSF enabled.
442238	FortiView VPN map can’t display Google map (199 dialup VPN tunnel).
442367	In *FortiView* > *Cloud Applications*, when the cloud users column is empty, drill down will not load.
483142	FortiView GUI dropped Threats shown as Session Allowed.

GUI

Bug ID	Description
408445	GUI test for secondary RADIUS server returns "invalid" secret, CLI test OK.
435780	GUI cannot delete SD-WAN rules or health-check.
451029	Should be able to assign hard token to user with no email configured by right clicking.
453706	If policy has `set fixedport enable` while using a `fixed-port-range` type IPpool, the session is dropped when dirty state hits.
462011	GUI is blank when accessed with RADIUS user with read-access profile and the FortiGate is managed by FortiManager.
464211	Some word cut off when changing widget size to 1*1 on dashboard.
468459	Translation issue on *Countries*.
468530	Can't set 2FA authentication and email recipient with `admingrp&usergrp` read-write on GUI.
469082	`prof_admin` profile admins are not able to display GUI IPv4 source address.
469666	While creating local users, the FortiGate GUI freezes, PC browser memory usage spikes, and the user is not created.
470452	Enhance FortiSwtich ports GUI to scale for larger switch networks.
472390	GUI won't load with ECC certificate selected.
474630	Central Management: IP/Domain Name disappears when using FQDN and clicking *Apply* causes management tunnel to go down.
474991	Cannot set Trust-IP as 0.0.0.0/24 on dedicated management interface via GUI.
475036	Virtual Server Duplicate Entry found Error on GUI.
475371	GUI *Edit Managed AP page* > *Firmware Upgrade* cannot recognize new images of FAP-221C, 222C, 223C, and 321C.
477592	Data shown under incorrect date in *Logs Sent to FortiAnalyzer Daily* graph.

Bug ID	Description
482897	If using a hyphen as a search character for DLP logs on GUI, unintended logs are included in the search result.
484303	No management IP info on GUI when VDOM is in TP mode.

HA

Bug ID	Description
474594	User cannot access the ForitGate management-ip through SSH.
474867	FortiGate does not send syslog from `ha-mgmt-interface` after `management-vdom` is changed
477392	Can't use FAC username and password and FortiToken two-factor authenticate login on HA slave unit.
482168	Ports are flapping when IPv6 traffic is passing through.
486552	Vcluster HA failover fails with large site-to-site IPsec VPN configuration on 3800D.

ICAP

Bug ID	Description
455779	User source IP in ICAP data packets.

IPS

Bug ID	Description
443418	User is not listed in quarantine list in case `block duration` value is set long enough.
450693	`ERR_SSL_PROTOCOL_ERROR` when deep scan enabled along with IPS in policy.
451452	IPS engine signal 14 alarm clock crash on FG-90D.
472980	System crashes after adding 199 custom IPS signatures.

IPsec VPN

Bug ID	Description
436301	Packets won't pass through IPsec tunnel after switching from static to dialup or from dialup to static.
453156	Suggest *net-device* and *tunnel-search* options setting can be changed.
461777	Sometimes kernel crash triggered by `diag vpn ike restart`.

Bug ID	Description
469648	Not all IPv6 IPsec VPN traffic work when crossing NP6.
474408	Multicast resolve wrong OIF for dialup VPN using `exchange-ip` to assign address (net-device enable).
491305	Packet from FortiClient cannot go through VXLAN over IPsec depending on packet size.

Log & Report

Bug ID	Description
438858	Synchronized log destination with *Log View* and *FortiView* display source.
468672	FG-3HD logs SIP traffic in the outbound direction while traffic is coming in the inbound direction.
476575	Filter result fields on compliance-check event log do not work.
491750	Log and SNMP Polling for `fnbamd` stats.

Proxy and WebProxy

Bug ID	Description
459972	WAD crashes when using external cache to store https objects.
467431	WAD treats `IPv6-addr` in Host Header as an invalid URL.
467709	High memory usage on WAD process with low session count.
471664	FG-1500D going into kernel conserve mode. WAD process consuming high memory.
473019	Web category cannot display on Web-proxy Block Page.
476391	Proxy AV breaks Citrix Virtual Delivery Agent (VDA) HTTP traffic.
482375	High memory usage on WAD.
484983, 487664	WAD SSL proxy crash with signal 11.
486821	Web application "Symphony" fails with AV profile enabled in policy.
489065	When user authentication/authorization fails, the username should be logged in the user event log.
489301	Some web proxy users receive Oops message with Error 504 Gateway timeout.
493272	Multiple WAD crashed with signal 11 (segmentation fault).
493470	Authenticated user receives Oops "Authentication requested" referencing a proxy policy which does not have authentication enabled.
494081	WAD process is crashing with signal 11 after upgrading firmware to 5.6.4.

Router

Bug ID	Description
458982	OSPF6 redistribute connected doesn't work as expected if area type is set as NSSA.
461660	OSPF nssa area redistributed IPv6 route cannot be learned properly by OSPF neighbor.
469131	Broadcast traffic getting forwarded when policy route is enabled in the device.
472512	FortiGate not forwarding DNS packets when policy route is hit and DNS filter profile is applied to firewall policy.
473972	When the X1 interface is brought down and back up, routing/BGP is lost even though there are no neighbours or routing to X1.
474083	SD-WAN Health check status shows interface down when the interface is up.
478307	SNMP reports incorrect MTU on GRE tunnels.
480978	OSPF summary-address synchronized with FGSP.
483443	VRRP start time option does not work when the VRRP primary device interface goes from down to up.

SSL VPN

Bug ID	Description
456027	SMB Bookmark in SSL VPN portal doesn't work with Dynamic user-mapping and getting error `Invalid HTTP request.`
458964	SSLVPN web mode SSH connection tool timeout in 5 minutes.
466821	Accessing *Cisco Unified Communications Manager* does not work properly.
471472	SSL VPN Duo authentication iframe does not load in 5.6 (Worked in v5.4).
472195	Request to increase Strict-Transport-Security HTTP Header `max-age=` value or make it configurable to pass security audit.
472541	Unable to log in to an internal website via SSL VPN web mode.
473963	SSL VPN web-portal allows access only to resources based on the first matched policy and its group.
483712	`sslvpnd` consumes high memory causing FortiGate to enter conserve mode.
484381	SSL VPN portal URL unreserved characters encoding issue.
486918	SSL VPN web mode unable to load the page correctly.
489827	On SSL VPN web mode, `Visteon.service-now.com/vss` URL does not load.

System

Bug ID	Description
395551	`cw_acd` restart every 1 minute on FG-800C.
415910	CPU cores utilization shows 0 percent while handling CPS in 5.4.
433745	SNMP trap & log for power failure with external redundant PSU.
436418	`inbandwidth` and `outbandwidth` of NP6lite interface does not work when offloaded.
442457	After deleting a LAG, FortiGate interface cannot be pinged.
459273	Slave worker blade loses local administrator accounts.
463982	FMG IP is unset in FGT CM.
465611	The sniffer's packet description does not show the source and destination IP for ESP traffic.
468938	Kernel panic on FG-3700D - Slave.
472561	FG-300E kernel panic once after factory reset.
474475	When unselecting member from an addrgrp via CLI, TAB completion allows you to see/unselect members that are not in the addrgrp.
475064	STP BPDUs not forwarded on ports connected to the internal switch of FG-3H0E.
475388	FG-501E, 10G Base-T transceiver doesn't work on SFP+ ports.
475692	System autoupdate schedule set time, setting mm to 60 for random does not work properly.
476446	Can't SSH to management interface if SSH is allowed only on the management interface.
477979	Potential memory leak detected in FTS.
479611	Cannot set the port associated with firewall address to virtual wire pair.
480411	DDNS does not work when dual wan is configured in `loadbalancing` mode.
482959	Unexpected system reboot with `comlog` output: soft lockup.
483014, 488587	FortiGate is rebooting at least once a day due to kernel panic.
483516	FG-81 enters conserve mode suddenly and `scanunit` crash.
484281	SALB cluster has synchronization issues.
486265	`check_sprite_file` timeout creates *tmpxxxxxx* files and causes FortiGate to enter conserve mode.
488222	Cannot use certificate for FortiGate administration.
488611	`virtual-wire-pair` IPv6 reflection session - ghost IPv6 sessions stacking in kernel/NP.
488861	Kernel panic and reboot.

User

Bug ID	Description
475294	Renewing expired guest account does not reset first login value.

VM

Bug ID	Description
408366	FGT_VM64 fails to join HA cluster after upgrade to b1117 (from b1111).
422241	FortiGate-VM Azure (BYOL & PAYG): Support for Azure Stack - Update WA Agent.
464434	WAN OPT is unavailable in FGT-VM GUI even when disk usage is set to wanopt.
486026	FortOS-VM On Demand stopped processing traffic after losing connection with FortiManager and was rebooted.
490280	Make the central management settings sticky after reboot.
491974	Possible memory leak in awsd.

WAF

Bug ID	Description
463468	Clients are unable to connect to mail server when WAF is enabled on the VIP policy.
477074	Inconsistent WAF behavior.

WCCP

Bug ID	Description
460383	*I see you* message sent from FortiGate WCCP contains an *Assignment Info* component which is not part of the RFC specification.

WiFi

Bug ID	Description
454634	Web filter `set warning-prompt per-domain` is warning per-category instead of per-domain.
462297	No support to enable WIDS through CLI for 2x2 platforms.
467517	High Latency when web filter is enabled in the policy in TP mode and the packet travels twice through the FortiGate.
475897	FortiGuard quota timer is running faster than it should.

Bug ID	Description
482970	FAP with MAC OUI 70-4C-A5 as mesh leaf cannot connect with FWF local radio as mesh root.
484556	URL filter does not match for right-hand matched URL when there is similar URL entry which includes – (dash).

Known Issues

The following issues have been identified in version 5.6.5. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Application Control

Bug ID	Description
435951	Traffic keeps going through the `DENY` NGFW policy configured with URL category.
448247	Traffic-shaper in shaping policy does not work for specific application category like as P2P.
487421	Application control violation page leaks private IP and hostname.

Firewall

Bug ID	Description
478360	IPv6 VIP does not translate IP address.

FortiGate-90E/91E

Bug ID	Description
393139	Software switch span doesn't work on this platform.

FortiGate 3815D

Bug ID	Description
385860	FG-3815D does not support 1GE SFP transceivers.

FortiSwitch-Controller/FortiLink

Bug ID	Description
304199	HA with FortiLink traffic loss – no virtual MAC.
357360	DHCP snooping may not work on IPv6.
369099	FortiSwitch authorizes successfully, but fails to pass traffic until you reboot FortiSwitch.
404399	FortiLink goes down when connecting to ForiSwitch 3.4.2 b192.

FortiView

Bug ID	Description
366627	FortiView Cloud Application may display incorrect drill down *File and Session* list in the *Applications View*.
368644	*Physical Topology: Physical Connection* of stacked FortiSwitch may be incorrect.
375172	FortiGate under a FortiSwitch may be shown directly connected to an upstream FortiGate.
408100	Log fields are not aligned with columns after drill down on FortiView and Log details.

GUI

Bug ID	Description
356174	FortiGuard `updategrp` read-write privilege admin cannot open FortiGuard page.
374844	Should show `ipv6` address when set `ipv6` mode to `pppoe/dhcp` on *GUI* > *Network* > *Interfaces*.
375383	If the policy includes the *wan-load-balance* interface, the policy list page may receive a javascript error when clicking the search box.
422413	Use API monitor to get data for FortiToken list page.
442231	Link cannot show different colors based on link usage legend in logical topology real time view.
445113	IPS engine 3.428 on Fortigate sometimes cannot detect Psiphon packets that iscan can detect.
451776	Admin GUI has limit of 10 characters for OTP.

HA

Bug ID	Description
458320	Cluster uptime was not consistent.
471816	Policy route setting is synced in `standalone-config-sync` mode.
493759	When vcluster2 is removed from HA configuration, all active sessions are killed once `session-ttl` is reached.

Log & Report

Bug ID	Description
412649	In NGFW Policy mode, FortiGate does not create webfilter logs.

Proxy

Bug ID	Description
454185	Specific application does not work when deep inspection is enabled.

Security Fabric

Bug ID	Description
403229	In FortiView display from FortiAnalyzer, the upstream FortiGate cannot drill down to final level for downstream traffic.
411368	In FortiView with FortiAnalyzer, the combined MAC address is displayed in the *Device* field.

SSL VPN

Bug ID	Description
405239	URL rewritten incorrectly for a specific page in application server.
477231	Unable to login to VMware vSphere Client 6.5 through SSL VPN web portal.
492066	High memory usage in SSL VPN even when there is only one connection.
495304	SSL VPN web portal with a bookmark pointing you to the website http://www.uptodate.com/contents/search is not working.

System

Bug ID	Description
295292	If `private-data-encryption` is enabled, when restoring config to a FortiGate, the FortiGate may not prompt the user to enter the key.
435388	After VLAN interfaces are added under physical interface, the parent interface cannot be added into a zone.
436580	`PDQ_ISW_SSE` drops at +/-100K CPS on FG-3700D with FOS 5.4 only.
436746	NP6 counter shows packet drops on FG-1500D. Pure firewall policy without UTM.
440411	Monitor NP6 IPsec engine status.
457096	FortiGate to FortiManager tunnel (FGFM) using the wrong source IP when multiple paths exist.
461580	Getting authentication portal by FQDN:1000/login? and /logout? does not work if using `auth-redirect fqdn` in policy.
464873	RADIUS COA Disconnect-ACK message ignore RADIUS server `source-ip` setting.
475745	Backup password for administrator account is not working when interface is down.

Bug ID	Description
486466	HTTPS web page is blocked after clicking *Proceed* button.
490066	FortiClient with IPsec with Proxy / Webfilter - Fragmentation is needed.
492193	DoS policies consume 20% more CPU than in FortiOS 5.2.

VM

Bug ID	Description
441129	Certify FortiGate-VMX v5.6 with NSX v6.3 and vSphere v6.5.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.